



NAVAL INVESTIGATIVE SERVICE

HOFFMAN BUILDING
2461 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22331

IN REPLY REFER TO
NIS-09X/kac
5420
Ser U-1566
25 June 1975

FOR OFFICIAL USE ONLY

MEMORANDUM FOR THE CHAIRMAN, SECURITY COMMITTEE, UNITED STATES
INTELLIGENCE BOARD

Subj: Security policy on travel and assignment of personnel with
access to sensitive intelligence

Encl: (1) Draft USIB policy paper on the above subject

1. This provides the report of the working group established by your predecessor at the 26 February 1974 meeting of the Security Committee to examine all factors bearing on and to develop a proposed USIB security policy for travel and assignment of personnel with access to sensitive intelligence. Enclosure (1), a draft of the recommended USIB policy, has the substantive concurrence of the representatives of CIA, DIA, Army, Navy, Treasury (Secret Service) and State. Representatives of FBI and ERDA abstained from participation in the working group as the subject was not of direct concern to their agencies. The representative of NSA non-concurs. He maintains that current DCI policy on travel and assignment is more meaningful and appropriate. The representative of Air Force also non-concurs. No alternative proposals to enclosure (1) have been provided by those agency representatives who have nonconcurred. Prolonged discussion of this matter has made it apparent that unanimity cannot be achieved in the working group.

2. Enclosure (1) was drafted with the intent of establishing a system susceptible of practical application by each USIB Principal which would:

a. Be consistent with current legal and societal limits on the restraints which may properly be put on an individual's private travel.

b. Provide a reasonable balance between operational requirements and security considerations without the necessity for large numbers of waivers.

c. Place reasonable limits on the type and extent of hazardous activities restrictions, and make their application the responsibility of each agency (including the military departments) for their own personnel.

d. Require Intelligence Community agencies to establish and maintain programs of security briefings for those traveling or being assigned to areas where there is an identified risk of interrogation, entrapment or capture.

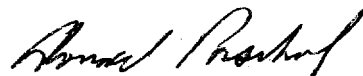


NIS-09X/kac
5420

e. Establish a uniform USIB policy for the protection of all sensitive intelligence, not limited to the community-wide compartmentation systems, and provide for ongoing support to the policy by the USIB Security Committee under the cognizance of the DCI. 25X1

25X1 3. Significant help in examining this problem was provided by [redacted] [redacted] formerly the Project Officer, CIA Risk of Capture Program. The wealth of information he provided on experiences of U.S. personnel captured or detained abroad was most useful in broadening our understanding of what has happened in the way of attempts to elicit sensitive intelligence from Americans. The facts he presented showed clearly that advance preparation in the form of appropriate briefings has enabled captured personnel to avoid providing sensitive information even under duress.

25X1 4. Basic USIB policy or travel and assignment with regard to community wide compartmentation systems generally was set forth in USIB-D-9.6/6 of 1 April 1963. Varying implementation of that policy within the [redacted] [redacted] systems led the CIA Special Security Center to draft a revised policy in late 1973. That draft revision provided for waivable restrictions of not more than a year for individuals with current access and was applicable only to areas where hostilities were in progress. It did not provide for any defensive briefing programs. It was withdrawn in the face of objections by NSA and others. Unsuccessful efforts to develop a "compromise" revision were followed by formation of the working group chaired by me. While the initiative on a revised policy rests with the Security Committee, I do not believe that the status quo can be maintained without possible legal challenge directed against the DCI and without the risks implicit in continuing divergence in individual agency security policies. I therefore strongly urge that this matter be referred to the Security Committee for resolution, and that a revised USIB policy be submitted to the Board for their approval. 25X1



DONALD PASCHAL
Working Group Chairman

Copy to:
Working Group Members

UNITED STATES INTELLIGENCE BOARD SECURITY POLICY
CONCERNING TRAVEL AND ASSIGNMENT OF PERSONNEL
WITH ACCESS TO SENSITIVE INTELLIGENCE

1. This establishes United States Intelligence Board security policy applicable to assignment and travel by personnel who have or have had access to sensitive intelligence (defined herein). Policy stated herein supersedes all previous intelligence community directives on this subject.^{1/}
2. Purpose. This policy is based on the need to protect sensitive intelligence information known to individuals from possible compromise resulting from their capture, interrogation or entrapment by hostile or unfriendly nations or groups. This policy is designed to limit the risk of compromise by providing security guidance to assist affected personnel in meeting their security responsibilities during unofficial travel and official assignments, and, in particular cases, by restricting official assignments.
3. Definitions. The following definitions apply for purposes of this policy:
 - a. Sensitive intelligence consists of intelligence information, sources and methods, which involve collection techniques particularly vulnerable to hostile counteraction if compromised and which are essential to the continued provision of intelligence needed for national security. Compartmented intelligence is included in the category of sensitive intelligence, and consists of all information and material bearing special community controls indicating restricted handling. Intelligence other than that

^{1/} Including those portions of the Communications Intelligence Security Regulation (attachment to DCID 6/3) which pertain to hazardous activity restrictions.

which is formally compartmented should be considered sensitive for purposes of this policy only when it is subject to special controls indicating restricted handling and limited access within individual intelligence community agencies.

b. Defensive security briefings are advisories to alert persons planning travel or assignment to certain areas of risks of acts of harassment, provocation or entrapment against them by local officials. Such briefings should be based on actual experience wherever feasible, and should include information on courses of action helpful in mitigating the adverse security and personal consequences of such acts.

c. Hazardous activities include, for areas where hostilities are taking place, duties in, over or under a combat zone or behind hostile lines, and duties in isolated or exposed areas where individuals cannot reasonably be protected against hostile action. Hazardous activities also include assignment or visits to or in the immediate vicinity of, and travel through, nations which have violated, or have threatened to violate, established norms of international law and usage applicable to innocent passage or the conduct of lawful, official business.

d. Risk of capture briefings are advisories to alert persons likely to engage in hazardous activities of what they may expect in the way of attempts to force or trick them to divulge classified information if captured or detained, and of suggested courses of action they should follow to avoid or limit such divulgence if they are captured, to include advance preparation of an innocuous, alternative explanation of their duties and background.

4. Policy Requirements. Security policies concerning travel and assignment shall provide for the following as a minimum:

a. All persons being granted or now holding access to sensitive intelligence shall be advised that they are required for the duration of access to: (1) give advance notice of planned travel to or through countries identified herein (Appendix A) as posing a security risk; (2) obtain a defensive security briefing before traveling to such countries whenever practical; (3) contact immediately the closest United States consular, attache or Embassy official if they are detained or subjected to significant harassment or provocation while traveling; and (4) report after return from travel any incidents of potential security concern which befell them. Individuals with continuing access should be reminded annually of these obligations through security education programs.

b. All persons whose access to sensitive intelligence is being or has been terminated shall be reminded of their security obligations for the continued protection of that intelligence, and shall be requested to comply with the provisions above for a stated period of time (not to exceed one year) after termination.

c. No person with access to sensitive intelligence should be officially assigned to hazardous activities without a thorough review of the nature and extent of his access balanced against operational requirements of having that particular person's services and talents available at a designated time and place. Where the individual reviews required hereunder indicate that the risk of compromise of sensitive intelligence outweighs operational benefits, restrictions against assignment to hazardous activities should

be imposed. Restrictions after termination of access may be imposed for not more than one year and then only when the individuals concerned had significant knowledge of sensitive intelligence sources and methods. When individual review shows that operational requirements outweigh the risk of compromise, persons subject to this policy shall be assigned to hazardous activities only after they have been given risk of capture briefings. Hazardous activities restrictions based on criteria herein should be applied individually by intelligence community departments and agencies to personnel assigned to, employed by, or in a contractual/consultant status with such departments and agencies.

5. Community Responsibilities

a. The DCI will cause to be prepared and disseminated to USIB members changes as necessary to the list of countries identified as posing a security risk bearing on this policy (Appendix A); and source material concerning the security risks to be guarded against by application of this policy. The USIB Security Committee will coordinate required support in these regards.

b. USIB Members will develop and apply security policies concerning travel and assignment consistent with the overall policy, criteria and definitions herein, to include:

(1) Preparing and providing to concerned personnel of their departments or agencies security education material on harassments or provocations against U.S. personnel traveling in or assigned to foreign nations or areas listed in Appendix A, with emphasis on acts which appear to represent attempts to compromise sensitive U.S. intelligence.

(2) Preparing and providing risk of capture briefings to personnel of their departments or agencies who are being assigned duties involving hazardous activities. Where necessary, applying hazardous activities restrictions on the assignment of their personnel; such restrictions to be approved by the Senior Intelligence Officer of each agency or department, to include the Military Departments. (Since the degree of risk for particular persons may vary with their status or employment, each USIB member should determine which of the countries listed in Appendix A should be categorized as hazardous for purposes of applying assignment restrictions and providing risk of capture briefings to personnel of their departments or agencies.)

(3) Insuring that new information obtained by their departments or agencies on harassments or provocations, or on risk of capture situations, is provided to the DCI and to other interested USIB agencies, and, where warranted by such new information, recommending changes to the list of countries posing a security risk (Appendix A).

c. Each USIB Member should insure that his policies in these regards consider the security requirements of sensitive intelligence programs known to his personnel which are managed or conducted by other Intelligence Community agencies.

APPENDIX A
TO
UNITED STATES INTELLIGENCE BOARD SECURITY POLICY
CONCERNING TRAVEL AND ASSIGNMENT OF PERSONNEL
WITH ACCESS TO SENSITIVE INTELLIGENCE

List of countries in which there is deemed to be a risk of harassment, provocation, entrapment, capture or detention of U.S. personnel posing a threat to the security of sensitive intelligence known to such personnel. All territory claimed or controlled by the listed countries is included, irrespective of whether the national boundaries involved are formally recognized by the United States Government.

Albania

Bulgaria

Cambodia

China (Peoples Republic of)

Cuba (except U.S. Naval Base, Guantanamo)

Czechoslovakia

German Democratic Republic (East Germany)

Hungary

Laos

Mongolia

North Korea (and adjacent Demilitarized Zone)

North Vietnam

Poland

Rumania

South Vietnam

Syria

USSR

Chinmen (Quemoy), Matsu and other islands offshore from mainland